

IN THE UNITED STATES DISTRICT COURT
FOR THE MIDDLE DISTRICT OF TENNESSEE
NASHVILLE DIVISION

DON JOLE)
)
v.) NO. 3-11-0882
) JUDGE CAMPBELL
LORI APPLE, et al.)

MEMORANDUM

Pending before the Court is Defendant Spriggs' Motion to Dismiss (Docket No. 16). For the reasons stated herein, Defendant's Motion to Dismiss is GRANTED in part and DENIED in part.

FACTS

Plaintiff's Complaint sets forth claims against Defendants Apple and Spriggs for alleged invasion of privacy, violation of state and federal electronic communications law, conversion and civil conspiracy. Plaintiff alleges that Defendants committed cybercrimes and torts against Plaintiff out of revenge because Plaintiff has severed a relationship with Defendant Spriggs and had spurned Defendant Apple's advances. Plaintiff contends, among other things, that Defendants conspired to access his Paypal account and his student loan account without authorization; to hack his computer and email account; to acquire personal and confidential information about Plaintiff and his family; and to burn his modeling portfolio and have him arrested for DUI.

Defendant Spriggs has moved to dismiss Count Three (violation of the Tennessee Wiretapping Act), Count Four (violation of the Tennessee Personal Commercial Computer Act) and Count Six (violation of the Computer Fraud and Abuse Act).

MOTIONS TO DISMISS

For purposes of a motion to dismiss, the Court must take all of the factual allegations in the complaint as true. *Ashcroft v. Iqbal*, 129 S.Ct. 1937, 1949 (2009). To survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to state a claim to relief that is

plausible on its face. *Id.* A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged. *Id.* Threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice. *Id.* When there are well-pleaded factual allegations, a court should assume their veracity and then determine whether they plausibly give rise to an entitlement to relief. *Id.* at 1950. A legal conclusion couched as a factual allegation need not be accepted as true on a motion to dismiss, nor are recitations of the elements of a cause of action sufficient. *Fritz v. Charter Township of Comstock*, 592 F.3d 718, 722 (6th Cir. 2010).

COUNT THREE: VIOLATION OF TENNESSEE WIRETAPPING ACT

The Tennessee Wiretapping Act (“TWA”) provides that a person commits an offense who intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept any wire, oral, or electronic communication. Tenn. Code Ann. § 39-13-601(a)(1)(A).

The TWA also provides that a person commits an offense who intentionally discloses or endeavors to disclose to any other person the contents of any wire, oral or electronic communication, knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of the law. Tenn. Code Ann. § 39-13-601(a)(1)(C). In addition, a person commits an offense who intentionally uses or endeavors to use the contents of any wire, oral or electronic communication knowing or having reason to know that the information was obtained through the interception of a wire, oral or electronic communication in violation of the law. Tenn. Code Ann. § 39-13-601(a)(1)(D). A person aggrieved by the violation of Section 39-13-601 may bring a civil action to recover money damages against the person engaged in that violation. Tenn. Code Ann. § 39-13-603.

The TWA defines “intercept” as the aural or other acquisition of the contents of any wire, electronic or oral communication through the use of any electronic, mechanical or other device. *Cardinal Health 414, Inc. v. Adams*, 582 F.Supp.2d 967, 979 (M.D. Tenn. 2008); Tenn. Code Ann. § 40-6-303(11). Unless an e-mail is actually acquired in its split second transmission over a computer network, it cannot be “intercepted” as that term is reasonably understood. *Id.* In other words, for a communication to be “intercepted,” it must be acquired during the “flight” of the communication. *Id.* Congress did not intend for “intercept” to apply to electronic communications when those communications were in electronic storage. *United States v. Steiger*, 318 F.3d 1039, 1048 (11th Cir. 2003); *see also Expert Janitorial, LLC v. Williams*, 2010 WL 908740 at * 6 (E.D. Tenn. Mar. 12, 2010) (finding that wiretap acts prohibit interception of emails acquired during flight of the communication is the correct approach).

Although Defendant Spriggs does not raise this issue, Plaintiff has not alleged that Defendant Spriggs actually intercepted any of Plaintiff’s communications during “flight.” At best, Plaintiff argues that because Defendant Spriggs allegedly engaged in unauthorized viewing of Plaintiff’s e-mail and text messages, she “had the opportunity to intercept Plaintiff’s electronic messages in real time.” Docket No. 21, p. 15. Thus, Plaintiff asks the Court to make a “reasonable inference” that Defendant Spriggs unlawfully “intercepted” Plaintiff’s communication in violation of this state statute. *Id.*

The Court finds that Plaintiff has not pled sufficient factual allegations that the emails at issue were obtained contemporaneously with their transmission. Therefore, Defendant Spriggs’ Motion to Dismiss Count Three is GRANTED.

COUNT FOUR - TENNESSEE PERSONAL AND COMMERCIAL COMPUTER ACT

Plaintiff alleges that Defendants' actions violated the Tennessee Personal and Commercial Computer Act ("TPCCA"), which provides, among other things, that whoever intentionally and without authorization, directly or indirectly, accesses any computer may be sued in a civil action for damages. Tenn. Code Ann. § 39-14-602(b)(1) and § 39-14-604. The TPCCA also provides a civil remedy against anyone who accesses computer software for the purpose of maliciously gaining access to computer material or to tamper maliciously with computer security devices or makes unauthorized copies of information produced by a computer. Tenn. Code Ann. § 39-14-602(b)(4) and (5).

Defendant Spriggs argues that only certain types of computer attacks are prohibited by this statute and that none of Plaintiff's allegations involves these kinds of attacks. Plaintiff's allegations do describe conduct, however, which could be found to violate the subsections (1), (4) and (5) cited above. The Court finds that Plaintiff has alleged sufficient facts concerning the violation of the TPCCA to survive a Motion to Dismiss. Defendant Spriggs' Motion to Dismiss Count Four is DENIED.

COUNT SIX - COMPUTER FRAUD AND ABUSE ACT

Defendant Spriggs contends that Count Six must be dismissed because the Computer Fraud and Abuse Act ("CFAA") applies only to "protected computers" and those are computers used by financial institutions and federal agencies and departments and computers used in interstate commerce. Defendant asserts that Plaintiff is neither a financial institution nor a federal agency and is not engaged in interstate commerce. Therefore, according to Defendant Spriggs, Plaintiff has not stated a claim for violation of the CFAA.

The statute defines “protected computer” as a computer exclusively for the use of a financial institution or the U.S. government or a computer which is used in or affecting interstate or foreign commerce or communication. 18 U.S.C. § 1030(e)(2); *Shurgard Storage Centers, Inc. v. Safeguard Self Storage, Inc.*, 119 F.Supp.2d 1121, 1125 (W.D. Wash. 2000). Plaintiff argues that any computer connected to the internet is a computer affecting interstate commerce.

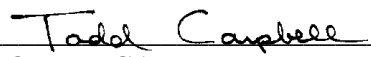
The Court agrees with those cases which have found that a connection to the internet is affecting interstate commerce or communication. *See, e.g., Continental Group, Inc. v. KW Property Mgmt., LLC*, 622 F.Supp.2d 1357, 1370 (S.D. Fla. 2009); *Paradigm Alliance, Inc. v. Celeritas Technologies, LLC*, 248 F.R.D. 598, 602 and n. 5 (D. Kan. 2008) (computer providing access to world-wide communications satisfies the element of interstate communications in the CFAA); and *United States v. Trotter*, 478 F.3d 918, 921 (8th Cir. 2007) (internet is an instrumentality and channel of interstate commerce).

For these reasons, the Court finds that Plaintiff has sufficiently alleged violation of the CFAA to survive the pending Motion to Dismiss and Defendant Spriggs’ Motion to Dismiss Count Six is DENIED.

CONCLUSION

Accordingly, Defendant Spriggs’ Motion to Dismiss (Docket No. 16) is GRANTED in part and DENIED in part. Plaintiff’s claim for violation of the Tennessee Wiretapping Act (Count Three) is DISMISSED.

IT IS SO ORDERED.


TODD J. CAMPBELL
UNITED STATES DISTRICT JUDGE